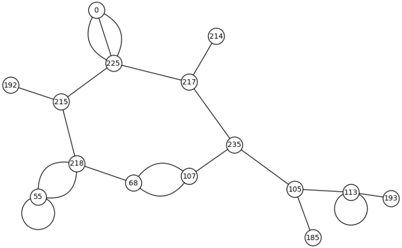
Adventures in Supersingularland: A Look at Supersingular Isogeny Graphs

Jana Sotáková

QuSoft / UvA

November 15, 2019, Amsterdam



Isogenies in post-quantum cryptography

Why should we care about isogenies?

We can do post-quantum crypto with isogenies:

1. SIKE (KEM, in the NIST competition),
2. CSIDH (key exchange),
3. signatures (SeaSign, CSI-FiSh),
4. other constructions (VDFs, threshold schemes, ...?)

The time to understand isogenies is now

About elliptic curves

Elliptic curves

They are given by an equation

$$y^2 = x^3 + ax + b \qquad \text{for some } a, b \text{ such that } 4a^3 + 27b^2 \neq 0$$

together with a point at infinity ∞.

In crypto

Usually, we ask that $a, b \in \mathbb{F}_p (= \mathbb{Z}/p$ finite field with p elements)
And that also $x, y \in \mathbb{F}_p$: clearly only finitely many solutions.

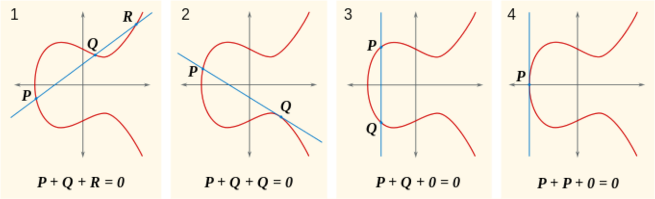
Fact

We can count the number of solutions $\#E(\mathbb{F}_p)$ efficiently.

Group law

Group law

1. add two points: draw a line through them, flip the third intersection point over the x-axis,
2. double a point: draw a tangent, flip the intersection point over the x-axis.



We want to understand $E[2] = \{P \in E : [2]P = \infty\}$.

Inverse of a point

If $P = (x, y)$ then $-P = (x, -y)$.
Hence points of order 2 satisfy $y = 0$.

Points of order 2

Need to find points for which $y = 0$.

$E : y^2 = x^3 - x$

Factor $x^3 - x = x \cdot (x-1) \cdot (x+1)$ so points of order 2 are:

$$P = (0,0),\ Q = (1,0),\ R = (-1,0)$$

$E : y^2 = x^3 - 2x$

Factor $x^3 - 4x = x(x^2 - 2)$. We still have 3 points of order 2 :

$$P = (0,0),\ Q = (\sqrt{2},0),\ R = (-\sqrt{2},0).$$

Fact

For any N, we have

$$E[N] = \{P : [N]P = \infty\} \cong \mathbb{Z}/N \times \mathbb{Z}/N$$

Isogenies

Algebraic formula for multiplication by 2:

Multiplication by [2] on the elliptic curve $y^2 = x^3 - x$ is given by:

$$\begin{aligned} P &\mapsto [2]P \\ (x, y) &\mapsto \left(\frac{x^4 + 2x^2 + 1}{4(x^3 - x)}, y \cdot \frac{8x^6 - 40x^4 - 40x^2 + 8}{64(x^3 - x)^2} \right) \end{aligned}$$

Not defined at ∞ and points where $x^3 - x = 0$:

$$\infty, P, Q, R \mapsto \infty$$
$$\ker[2] = \{\infty, P, Q, R\} = E[2]$$

Properties:

1. group homomorphism,
2. given by algebraic formulas,
3. has a finite kernel.

Isogenies: a definition

Definition of isogenies

A map $\phi : E \to E'$ of elliptic curves is an isogeny if:

- it is given by rational functions in the coordinates x, y on E,
- preserves the group law of elliptic curves,
- has a finite kernel (which is always a subgroup). In particular, only finitely many points map to ∞.

The degree of the isogeny ϕ is defined to be $\# \ker \phi$.

Existence of isogenies

For any finite subgroup H, there exists an isogeny $\phi : E \to E'$ with kernel exactly H:

$$E \to E' =: E/H$$

and there are formulas for it.

Isogenies have a factoring property

Isogenies have a universal property:

Let $\phi : E \to E'$ be an isogeny. If $P \in \ker \phi$, then there exist isogenies ψ, φ such that $\ker \psi = \langle P \rangle$ and

$$\phi = \varphi \circ \psi$$
$$\deg \phi = \deg \varphi \cdot \deg \psi$$

$$\begin{tikzcd}
E \arrow[rr, "\phi"] \arrow[dr, "\psi"] & & E' \\
& \tilde{E} \arrow[ur, "\varphi"] &
\end{tikzcd}$$

Isogenies have a factoring property

Isogenies have a universal property:

Let $\phi : E \to E'$ be an isogeny. If $P \in \ker \phi$, then there exist isogenies ψ, φ such that $\ker \psi = \langle P \rangle$ and

$$\phi = \varphi \circ \psi$$

$E : y^2 = x^3 - x$ and $\phi = [2]$ multiplication by 2

Then $(0,0) \in \ker[2] = \{\infty, (0,0), (1,0), (-1,0)\}$ and

$$\begin{tikzcd}
E \arrow[rr, "\left(\frac{x^4+2x^2+1}{4(x^3-x)}, \frac{8x^6y-40x^4y-40x^2y+8y}{64(x^6-2x^4+x^2)}\right)"] \arrow[dr, "\psi", "\left(\frac{x^2-1}{x}, \frac{x^2y+y}{x^2}\right)"'] & & E \\
& y^2 = x^3 + 4x \arrow[ur, "\hat{\psi}"', "\left(\frac{\frac{1}{4}x^2+1}{x}, \frac{\frac{1}{8}x^2y-\frac{1}{2}y}{x^2}\right)"] &
\end{tikzcd}$$

One can check that $\hat{\psi} \circ \psi = [2]$ by composing the formulae.

Detour on the j-invariant

The factorization is unique up to composing with isomorphisms of elliptic curves.
For an elliptic curve

$$E : y^2 = x^3 + ax + b$$

define j-invariant $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2} \in \mathbb{F}_{p^2}$.

$E : y^2 = x^3 - x$
has $b = 0$ and so $j(E) = 1728$.

j-invariant

is an isomorphism invariant: if E and E' can be obtained from each other by a change of coordinates then

$$j(E) = j(E').$$

Small recap

So far

1. There are always 3 isogenies of degree 2,
2. we can compute them efficiently using Vélu's formulas.

Points of larger degree

Let P be a point on $E(\mathbb{F}_p)$ of order N, assume $N = 2^n$.

1. There is an isogeny of degree 2^n with $\ker\phi = \langle P\rangle$:

$$\phi : E \to E' = E/\langle P\rangle$$

2. But Velu's formulas are no longer efficient.
3. but $Q = [2^{n-1}]P$ has order 2 and we can decompose:

$$\begin{tikzcd}
E \arrow[rr, "\text{deg}=2^n", "\phi"'] \arrow[dr, "\psi", "\text{deg}=2"'] & & E/\langle P\rangle \\
& E/\langle Q\rangle \arrow[ur, "\text{deg}=2^{n-1}"'] &
\end{tikzcd}$$

Isogeny-based Diffie-Hellman

set-up

Choose an elliptic curve E defined over some $\mathbb{F}_q$ that satisfies that $E[2^r], E[3^s] \subset E(\mathbb{F}_q)$.

1. Alice chooses a secret $P \in E[2^r]$ and computes the isogeny $\phi_A : E \to E/\langle P \rangle =: E_A$
2. Bob chooses a secret $Q \in E[3^s]$ and computes $\phi_B : E \to E/\langle Q \rangle =: E_B$
3. Alice and Bob exchange E_A, E_B ($+$ a bit more of extra information)
4. They both are able to compute $j(E_{AB}) = j(E/\langle P, Q \rangle)$.

$$
\begin{tikzcd}
E \arrow[r, squiggly, "\text{Alice using her secret}"] \arrow[d, squiggly, "\text{Bob}"'] & E_A \arrow[d, squiggly, "\text{Alice using Bob's public key}"] \\
E_B \arrow[r, squiggly, "\text{Bob}"'] & j(E_{AB})
\end{tikzcd}
\qquad (\leftarrow \text{ shared key})
$$

Finally, isogeny graphs

Alice's secret is an isogeny $\phi_A : E \to E/\langle P \rangle$ of degree 2^r. We saw we can decompose this into a sequence of a isogenies of degree 2.

Definiton of an ℓ-isogeny graph

Let $\mathbb{F}_q$ be a finite field. Let S be a set of isomorphism classes (or j-invariants) of elliptic curves defined over $\mathbb{F}_q$. We define the following graph $G_\ell(\mathbb{F}_q)$:

- the set of vertices is S,
- there is an edge between $j, j' \in S$ if and only if there is a ℓ-isogeny between curves with j-invariants j and j'.

For Alice's secret to be safe

it needs to be difficult to find paths between the vertices $j(E)$ and $j(E_A)$ in the graph $G_2(\mathbb{F}_q)$.

Same for Bob in $G_3(\mathbb{F}_q)$.

Supersingular elliptic curves

We choose to use supersingular elliptic curves:

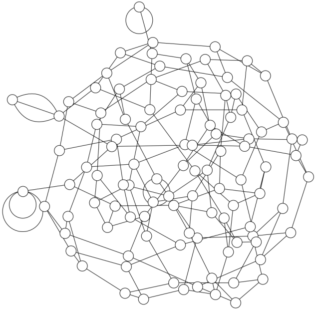
1. all supersingular elliptic curves have j-invariant in $\mathbb{F}_{p^2}$, and hence have equations over $\mathbb{F}_{p^2}$,
2. all supersingular elliptic curves have $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$ so if we choose
$$p = 2^r \cdot 3^s - 1,$$
we obtain $E[2^r]$ and $E[3^s]$ already defined over $\mathbb{F}_{p^2}$
3. so there are $3 \cdot 2^{r-1}$ different choices for Alice and $4 \cdot 3^{s-1}$ different choices for Bob.
4. moreover, path finding seems to be hard.

Supersingular isogeny graphs

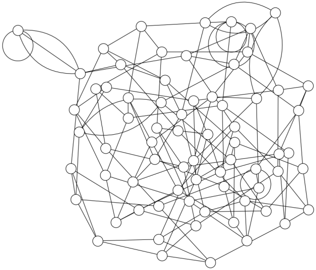
Supersingular ℓ-isogeny graphs $G_\ell(\mathbb{F}_{p^2})$

Vertices: all supersingular j-invariants.

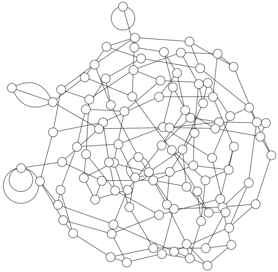
$p = 1223$ and $\ell = 2$

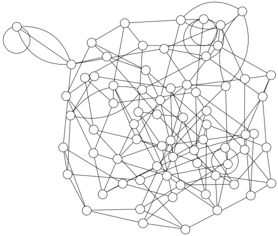


$p = 827$ and $\ell = 3$



Examples and properties



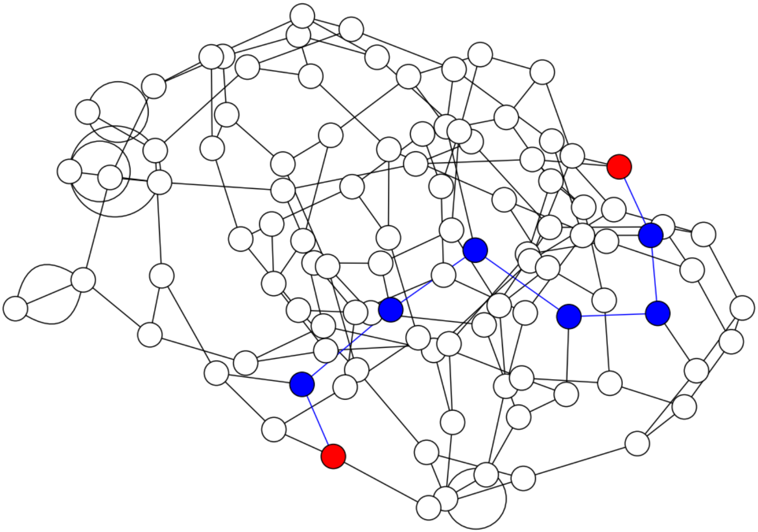


Properties

1. exponentially-large graphs ($\approx p/12$ vertices)
2. connected, $\ell + 1$-regular graphs (except for at most 2 vertices),
3. short diameters: $d = \Theta(\log(p))$,
4. expander graphs: taking random walks of length $\log(p)$ is almost as good as uniform sampling of vertices
5. path finding is hard (exponentially hard both classically and quantumly)

Path finding

For $p = 1223$ and $\ell = 2$, shortest path between two random vertices:



The Spine of $G_\ell(\mathbb{F}_{p^2})$

Path finding is not hard for all pairs of vertices

Between vertices labelled with j-invariants $j \in \mathbb{F}_p$, path finding is easier (subexponential).

Definition

The **spine** $\mathcal{S}$ is the induced subgraph with vertices

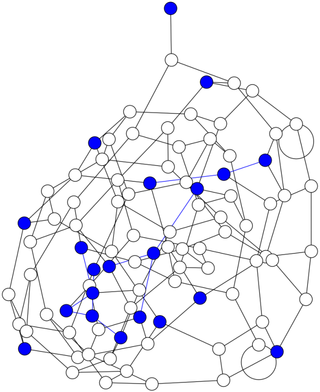
$$\{j : j \in \mathbb{F}_p\}$$

It is a subgraph of size approximately $\sqrt{p}$.

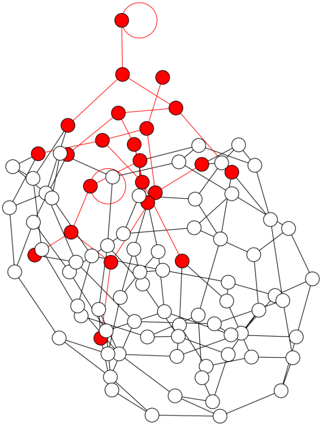
How do these vertices sit inside the graph?

For crypto, we usually assume that they are randomly distributed throughout the graph.

$p = 1103$, random subgraph of the expected size

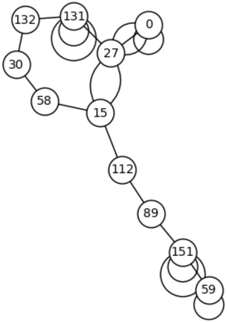


$p = 1103$, the subgraph of $\mathbb{F}_p$ vertices

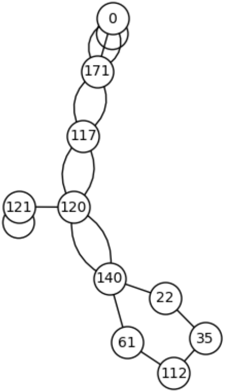


Examples of the spine

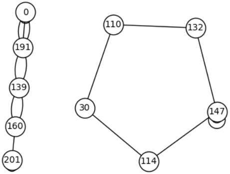
The spine for $\ell = 3$



$p = 167$



$p = 179$



$p = 227$

Visible structure

In the last picture, we see the nice cycle with 5 vertices and another component also with 5 vertices.

The CSIDH-land: the graph $\mathcal{G}_\ell(\mathbb{F}_p)$

Fix ℓ a small prime and p a large prime.

Definition of $\mathcal{G}_\ell(\mathbb{F}_p)$

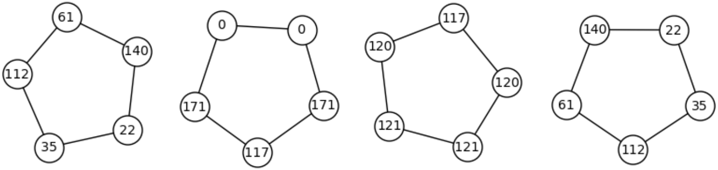
1. vertices: elliptic curves defined over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism,
2. edges: ℓ-isogenies defined over $\mathbb{F}_p$.

j-invariants

is not an $\mathbb{F}_p$-isomorphism invariant, every j-invariant will be there twice! (#quadratictwists)

Example with $p = 179$ and $\ell = 3$

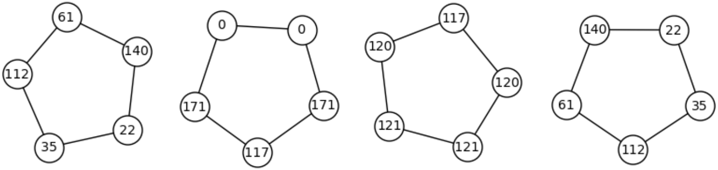
labels = j-invariants of the curves



Quick road to the CSIDH

Example with $p = 179$ and $\ell = 3$

labels = j-invariants of the curves



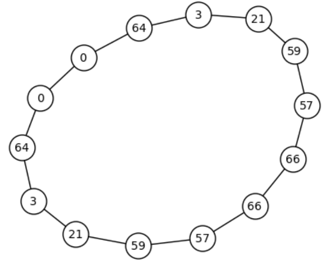
1. Any ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$ for $\ell > 2$ will be a union of cycles,
2. their sizes can be explained by class-group actions of $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$,
3. this abelian group actions makes navigation between vertices of these graphs subexponential
4. CSIDH takes a union of the graphs for several ℓ and argues that subexponential does not mean practical.

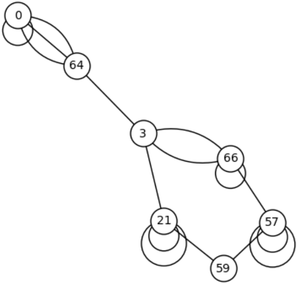
How to pass from $\mathcal{G}_\ell(\mathbb{F}_p)$ to the Spine $\mathcal{S}$

Two-step process

1. Identify vertices with the same j-invariant,
2. add edges that were not defined over $\mathbb{F}_p$.

For $\ell = 3$ and $p = 101$



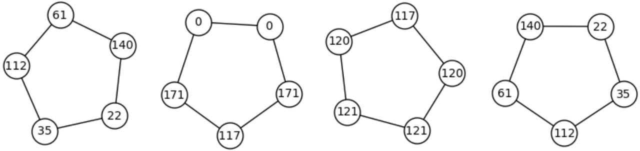


Lemma

Whenever we add an edge that does not correspond to an isogeny defined over $\mathbb{F}_p$, we get a double edge.

Neighbours

$\mathcal{G}_\ell(\mathbb{F}_p)$ for $p = 179, \ell = 3$



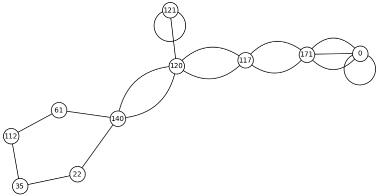
The Neighbour Lemma

Whenever the two vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ with j-invariant a do not have the same neighbours,

$$a = 1728.$$

Moreover, the two neighbours of one vertex with $j = 1728$ have the same j-invariant.

For $p = 179$, we have $1728 \equiv 117$ and we see the two double edges from 1728.



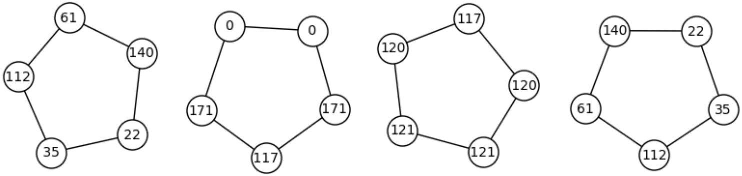
Main theorems

Let p be a prime such that the primes above ℓ in $(-4p)$ have odd order (i.e., all the connected components are cycles containing an odd number of vertices).

Theorem for $\ell > 2$

In the graph $\mathcal{G}_\ell(\mathbb{F}_p)$:

1. *for any connected component V of $\mathcal{G}_\ell(\mathbb{F}_p)$ that does not contain 1728, there exists a 'twist' component W such that if we consider V, W as cycles labelled by the j-invariants, V and W become identical,*

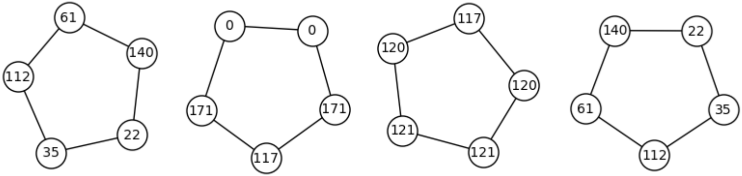


For $p = 179$ and $\ell = 3$, we have $1728 \equiv 117$.

Main theorems, continued

2. *the connected components of* 1728 *are symmetric: the vertices farthest away from* 1728 *are two curves with the same j-invariants connected by an ℓ-isogeny.*

   This is the only arrangement in which:
   - two vertices with the same j-invariant share an edge,
   - two components include vertices with the same j-invariant without being identical as in (1.)

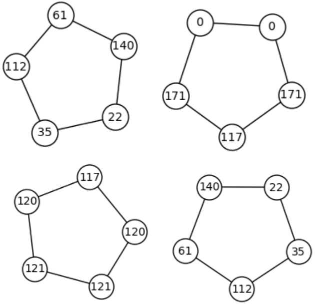


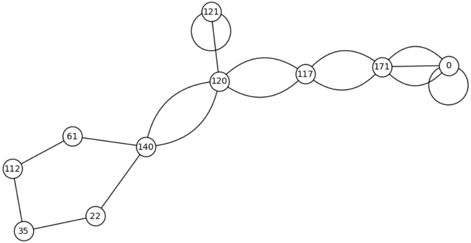
For $p = 179$ and $\ell = 3$, we have $1728 \equiv 117$.

Main theorems, continued a bit longer

When we pass to the spine $\mathcal{S}$, the following happens:

1. the two components containing 1728 first collapse into simple paths with 1728 at one end and with a loop at opposite ends,
2. these two looped-paths are then attached at the vertex 1728,
3. all other components get identified with their twist twins and form perfect cycles,
4. fewer than $4\ell^2$ new edges are added, and the newly-added edges always come in pairs.

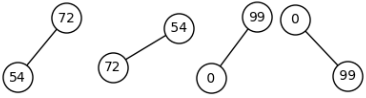




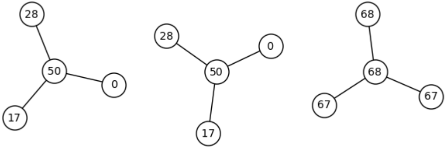
2-Isogenies: the graph $\mathcal{G}_2(\mathbb{F}_p)$

It depends on p mod 8:

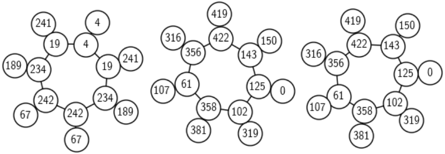
1. $p \equiv 1 \bmod 4$: bunch of edges



2. $p \equiv 3 \bmod 8$: claws



3. $p \equiv 7 \bmod 8$: volcanoes

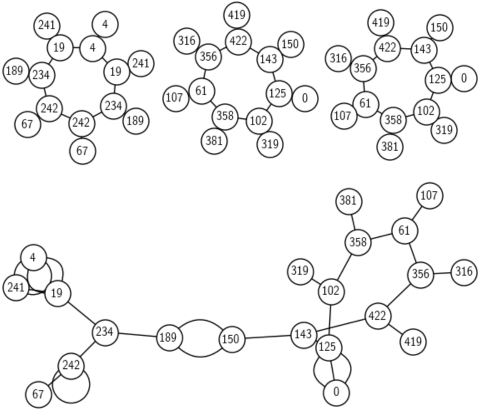


Example for $\ell = 2$ and $p = 431$

Example

The graph above is $\mathcal{G}_2(\mathbb{F}_p)$ and the graph below is the spine in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$.

We have
$1728 \bmod 431 = 4$
$8000 \bmod 431 = 242$
and 189 and 150 are the two roots of the polynomial $(X^2 + 191025X - 121287375)$ that we saw as a factor of $\mathrm{Res}_2(X)$.



Summary of what the Spine looks like for $\ell = 2$

The $\mathbb{F}_p$-subgraph $\mathcal{S} \subset \mathcal{G}_2(\overline{\mathbb{F}}_p)$:

1. for $p \equiv 1 \bmod 4$, we see single edges, with a possible vertex with a loop at $j = 8000$ and one possible component of size 4,
2. for $p \equiv 3 \bmod 8$, we see claws, with one claw collapsed to an edge ($j = 1728$), and a possible pair of claws joined by a double edge,
3. for $p \equiv 7 \bmod 8$, we see volcanoes, one of the volcanoes will be collapsed and possibly two volcanoes will get attached by a double edge to form a large component.

Thank you for your attention!

For more, go to: eprint 2019/1056